

Appl. No. 09/390,362
Reply to Office Action of: November 21, 2006

REMARKS

Applicant wishes to thank the Examiner for reviewing the present application.

Claim Amendments

Claim 14 is added, which is directed to a method for authenticating a communication between first and second correspondents, and includes the steps recited in both claim 1 and claim 7. As such claim 14 does not add any additional subject matter to be searched. Its purpose is to provide a linking claim combining those steps recited in sub-combinations directed to the signing and verification aspects of the authentication (i.e. claim 1 and claim 7 respectively).

Accordingly, no new subject matter is believed to have been added by way of this amendment.

Election/Restriction

The Examiner has requested a restriction of the claims under 35 U.S.C. § 121 to one of two allegedly distinct inventions, namely:

- I. Claims 1-6 and 11-13 to a signature generation method; and
- II. Claims 7-10 to a signature verification method.

Applicant elects the restriction of the claims to invention I with traverse.

The Examiner has requested restriction on the basis that "In the instant case, subcombination I has separate utility such as forming a signature having three components. Subcombination II has separate utility such as verifying authenticity of a message by examining a signature having two components". Applicant believes that the Examiner has erred in requiring restriction as follows.

According to MPEP § 803, there are two criteria for a proper requirement for restriction between patentably distinct inventions, namely (A) the inventions must be independent or distinct as claimed; and (B) there must be a serious burden on the Examiner if restriction is required.

Firstly, regarding criterion (A), the Examiner believes that the two groupings above are independent. However, according to MPEP 802.01, the term independent means that: "there is

Appl. No. 09/390,362
Reply to Office Action of: November 21, 2006

no disclosed relationship between the two or more subjects disclosed, that is, they are unconnected in design, operation, or effect...".

In the present application, groups I and II are clearly related in that the message signed, e.g. according to claim 1, is verified, e.g. according to claim 7. It is well known in the field of cryptography that for a signature to be verified a signature must have first been generated, i.e. there is an inherent relationship between signing and verification of a signature/message. Clearly signature generation and the corresponding verification of the signature should be considered at the same time. Applicant believes that for this reason alone the claims of the present application are related and thus connected in operation and effect. In fact, group I and group II are classified in the same class (713) by the Examiner and are given only separate sub-classifications. Therefore, a search under only a single classification is and has been required.

Applicant also notes that although claim 7 utilizes two components whereas claim 1 involves generating three components, the first component *c* in claim 7 is formed similar to how it is formed in claim 1 (see preamble of claim 7) and the plaintext bit string *V* is also part of a message that is split similar to how it is split in claim 1. Moreover, both claim 1 and claim 7 require that bit string *H* be hidden in component *c*.

It is well known in the field of cryptography that the components generated when forming a signature are not all necessarily used in verifying the signature. The common aspect of hiding plaintext bitstring *H* in component *c*, and the fact that component *c* is computed in a similar manner in both claim 1 and claim 7 clearly evidences a relationship between the above groupings. Applicant believes that the Examiner has not fully considered this relationship between claim 1 and claim 7 and in particular has overlooked those common elements discussed above. For this reason, Applicant believes that restriction is improper.

Secondly, regarding criterion (B), if the search and examination of an entire application can be made without serious burden, the Examiner must examine it on the merits, even though it may include independent or distinct claims (see MPEP section 803). Applicant respectfully submits that no such burden exists.

In the present application, claims 1-13 have been previously been examined together on the merits. For at least this reason, there is clear evidence that there is no serious burden in examining both the signature generation aspect and the signature verification aspect in the same application. Applicant believes that if the Examiner believed there was an undue burden, he

Appl. No. 09/390,362

Reply to Office Action of: November 21, 2006

should have made such a restriction before originally examining the present application. It is inappropriate to raise this issue for the first time after several office actions and the filing of a continuing examination. Since the MPEP makes it clear that there is a subjective determination to be made (undue burden) by the Examiner, the Examiner should also consider the undue burden on the Applicant by belatedly raising this issue. It is entirely within the discretion of the Examiner to determine the appropriateness for restriction and in doing so should be consistent with previous conduct on this file.

The Examiner contends that Applicant's previous amendments necessitated the restriction requirement. However, as noted above, the Examiner's specific reason that claim 1 and claim 7 are independent is that claim 1 involves forming three signature components and claim 7 involves operating on two signature components.

Applicant notes that claim 7 has previously required operation on only two signature components and claim 1 has previously involved forming three signature components. Therefore, Applicant believes that the Examiner's reason is unfounded and that even if this reason were to form the basis for requiring restriction of the claims, the issue should have been raised before undergoing substantive examination. Not only has examination already been conducted on the basis of claim 1 and claim 7 at the same time (in fact in more than one office action), the claims have always been related as discussed above. As such, there has clearly been no serious burden in examining claim 1 and claim 7 together and there would be no serious burden to continue to examine the claims together.

Applicant also notes that the previous amendments were to clarify the nature of the steps and in no way changed the number of signature components operated on in claim 7. This is believed to further evidence that restriction at this point during examination is improper.

Finally, as noted above, Applicant has added claim 14 which includes those steps performed by both the signing entity and the verifying entity and thus is a combination of claims 1 and 7. By virtue of this claim, the present application must be examined while taking into account both the signing and verification steps. Therefore, claim 14 is believed to link claims 1 and 7 as a combination of the two sub-combinations and thus would render any future restriction improper.

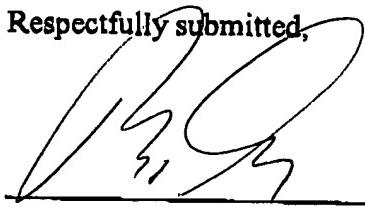
In view of the foregoing, Applicant respectfully submits that not only have the two prerequisites to proper restriction not been met, claim 14 has been added that requires the steps

Appl. No. 09/390,362
Reply to Office Action of: November 21, 2006

performed in both sub-combinations identified by the Examiner. Therefore, Applicant respectfully requests that the Examiner reverse the restriction requirement and continue to examine both groupings in the same application.

Applicant requests early reconsideration and allowance of the present application.

Respectfully submitted,



Ralph A. Dowell
Attorney for Applicant
Registration No. 26,868

Date: 12/18, 2006

Dowell & Dowell, P.C.
Suite 406
2111 Eisenhower Avenue
Alexandria, VA 22314
USA

Tel: (703) 415-2555
Fax: (703) 415-2559